CLAIMS

What is claimed is:

1. A method for controlling access to a computer system comprising:

classifying applications running on an untrusted computer system as running in one of a trusted application execution context and an untrusted application execution context; and

preventing an application on said untrusted computer system from initiating a connection with a trusted computer system unless said untrusted computer system is running said application in said trusted application execution context.

2. The method in claim 1, wherein said trusted computer system can initiate connections with any execution context on said untrusted computer system.

3. The method in claim 1, wherein only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system.

4. The method in claim 1, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

5. The method in claim 4, wherein a human administrator of said untrusted system assigns said distinctive application execution context names.

6. The method in claim 4, wherein said applications cannot change the names of respective execution contexts in which said applications are running.

7. The method in claim 4, wherein said applications cannot change the name of any execution context in said untrusted computer system.

8. The method in claim 1, wherein connections originating on said external system can terminate only at said untrusted system and only at said untrusted execution contexts therein.

9. The method in claim 1, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system.

10. A method for controlling access to a trusted computer system comprising:

determining a name of an execution context of an application running on an untrusted system;

determining whether said execution context is trusted or untrusted based on said name;

if said execution context is trusted, permitting said application to initiate a connection with said trusted system, and

if said execution context is untrusted, preventing said application from initiating a connection with said trusted computer system.

11. The method in claim 10, wherein said trusted computer system can initiate connections with any execution context on said untrusted computer system.

12. The method in claim 10, wherein only said untrusted application execution contexts on said untrusted system can initiate connections with an external computer system.

13. The method in claim 10, wherein said execution context name was previously assigned by a human administrator.

14. The method in claim 10, wherein there are a plurality of applications running on said untrusted computer system, one of said applications having a trusted execution context and another of said applications having an untrusted execution context.

15. The method in claim 14, wherein said applications cannot change names of the respective execution contexts in which said applications are running.

16. The method in claim 14, wherein said applications cannot change the name of any execution context in said untrusted computer system.

17. The method in claim 10, wherein connections originating on an external system can terminate only at said untrusted system and only at said untrusted execution contexts therein.

18. The method in claim 10, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system.

19. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform a method for controlling access to a computer system, said method comprising:

classifying applications running on an untrusted computer system as running in one of a trusted application execution context and an untrusted application execution context; and

preventing an application on said untrusted computer system from initiating a connection with a trusted computer system unless said untrusted computer system is running said application in said trusted application execution context.

20. The program storage device in claim 19, wherein said trusted computer system can initiate connections with any execution context on said untrusted computer system.

21. The program storage device in claim 19, wherein only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system.

22. The program storage device in claim 19, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

23. The program storage device in claim 22, wherein a human administrator of said untrusted system assigns said distinctive application execution context names.

24. The program storage device in claim 22, wherein said applications cannot change names of respective execution contexts in which said applications are running.

25. The method in claim 22, wherein said applications cannot change the name of any execution context in said untrusted computer system.

26. The program storage device in claim 19, wherein connections originating on said external system can terminate only at said untrusted system only at said untrusted execution contexts therein.

27. The program storage device in claim 19, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution contexts cannot interrogate or change critical system data of said untrusted computer system.

28. A system for controlling access to a network comprising:

a trusted computer system;

an untrusted computer system connected to said trusted computer system and to an external computer system,

wherein said untrusted system includes applications classified as having trusted application execution contexts and untrusted application execution contexts, and

wherein only said trusted application execution contexts can initiate connections with said trusted computer system.

29. The system in claim 28, wherein said trusted computer system can initiate connections with any execution context on said untrusted computer system.

30. The system in claim 28, wherein only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system.

31. The system in claim 28, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

32. The system in claim 31, wherein a human administrator of said untrusted system assigns said distinctive application execution context names.

33. The system in claim 31, wherein said applications cannot change the names of respective execution contexts in which said applications are running.

34. The method in claim 31, wherein said applications cannot change the name of any execution context in said untrusted computer system.

35. The system in claim 28, wherein connections originating on said external system can terminate only at said untrusted system and only at said untrusted execution contexts therein.

36. The system in claim 28, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system.